EMAIL SECURITY: SOCIAL ENGINEERING REPORT

How prepared are you to defend against social engineering attacks such as spear phishing, business email compromise and ransomware attacks?
Forty-six percent of surveyed security leaders say their organizations have been victimized by at least one targeted social engineering attack in the past year. And 52 percent rate their organizations’ defenses against targeted attacks at average or below.

These are among the results of the 2016 Social Engineering Report, sponsored by Agari, and they underscore the criticality of the FBI’s own recent update on today’s most insidious form of targeted attack – business email compromise.

According to the FBI, between Oct. 2013 and May 2016, law enforcement globally received 22,143 reports of business email compromise, which resulted in $3.1 billion in fraud losses. Since Jan. 2015, the FBI has seen a 1300 percent increase in victims and losses.

It couldn’t be clearer: Social engineering is the lever that fraudsters are using to penetrate organizations and commit big-dollar crimes – and no amount of anti-virus protection is going to defend against these sophisticated targeted attacks.

In the wake of the FBI report, this study was conducted to determine:

• The prevalence of social engineering attacks on U.S. organizations;
• The toll these attacks are exacting;
• The most effective controls for defending against these targeted strikes.

Read on to learn more. And pay special attention to our survey analysis at the end of this report, where we offer expert insight from Agari Field CTO John Wilson on how to best put these survey results to work to improve your organization’s defenses against targeted social engineering attacks.

Best,

Tom Field
Vice President, Editorial
Information Security Media Group
tfield@ismgcorp.com
This survey was conducted online in the summer of 2016, and it generated more than 200 responses from organizations across industrial sectors in the U.S. Respondent organizations were primarily in the healthcare, government, financial services and education sectors. Thirty-two percent of them employ 10,000 or more employees, and 42 percent have more than $1 billion in annual revenue.

Introduction .................................................................................... 2
By the Numbers: Stats About Social Engineering ......................... 4
Survey Results
   Social Engineering Baseline .......................................................... 5
   Attack Volumes & Types ............................................................... 8
   Trust & Defenses ........................................................................... 11
   Partner Vulnerability ..................................................................... 14
   Countermeasure Agenda ............................................................... 16
Conclusions ..................................................................................... 18
Survey Analysis
   John Wilson, Field CTO, Agari ..................................................... 19

About the Sponsor:

Agari, a leading cybersecurity company, is trusted by leading Fortune 1000 companies to protect their enterprise, partners and customers from advanced email phishing attacks. The Agari Email Trust Platform™ is the industry’s only solution that “understands” the true sender of emails, leveraging the company’s proprietary, global email telemetry network and patent-pending, predictive Agari Trust Analytics to identify and stop phishing attacks. The platform powers Agari Enterprise Protect, which help organizations protect themselves from advanced spear phishing attacks, and Agari Customer Protect, which protects consumers from email attacks that spoof enterprise brands. Agari, a recipient of the JPMorgan Chase Hall of Innovation Award and recognized as a Gartner Cool Vendor in Security, is backed by Alloy Ventures, Battery Ventures, First Round Capital, Greylock Partners, Norwest Venture Partners and Scale Venture Partners. Learn more at http://www.agari.com and follow the company on Twitter @AgariInc.
By the Numbers: Stats About Social Engineering

Offered as context for this report, the U.S. Federal Bureau of Investigation defines business email compromise – the latest manifestation of social engineering attacks – as “a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.”

In April 2016, the FBI released its latest statistics on incidents and losses attributed to business email compromise. Among the telling stats:

• 270% – increase in identified victims and exposed loss since Jan. 2015.
• $2.3 billion – global fraud losses from these crimes since Oct. 2013.

To complement those numbers, here are some compelling statistics from the 2016 Social Engineering Report:

• 60% of survey respondents say social engineering is one of the most significant threats they face today.

• 60% know they were or may have been victims of a social engineering attack in the past year.

• 65% of those who were attacked say that employees’ credentials were compromised as a result of these incidents.
Social Engineering Baseline

This opening section of the report reviews the general impact of social engineering on organizations today and gives survey respondents the opportunity to assess their organizations’ general defenses. Among the standout statistics:

- 46 percent of security leaders know their organizations were victim of at least one successful social engineering attack in the past year (14 percent are unsure);
- Only 5 percent rate their organizations' social engineering defenses as “superior.”

Read on for full baseline results.

**On a scale of 1-4, how do you categorize spear phishing* as a serious business threat to your organization?**

- It is one of the most significant threats we face today: 61%
- It is of some concern but not a top cybersecurity priority: 34%
- It is not perceived as a serious business threat: 4%
- We have not experienced spear phishing attacks: 1%

The message has taken root. Security leaders understand the criticality of social engineering, including spear phishing, as a business threat. As the chart shows, 94 percent of respondents say this is one of the most significant threats today, or at least of some concern. Only four percent say social engineering is not perceived as a serious business threat.

*In the survey, the term “spear phishing” was used in the questions instead of the more general and accurate term “social engineering,” which includes spear phishing, business email compromise and ransomware. This was done due to the greater general familiarity with the term “spear phishing” among the respondents.*
Survey Results

How do you assess your organization’s overall ability to defend against spear phishing attacks that target specific individuals to steal credentials and/or commit fraud?

- A - Superior: 5%
- B - Above average: 42%
- C - Average: 42%
- D - Below average: 9%
- F - Failing: 1%

Asked to generally assess their organizations’ ability to defend against social engineering attacks, 47 percent rate themselves as above average or superior. But that number is overshadowed by the 53 percent who rate their defenses at average or below. At a time when entities worldwide are losing billions of dollars to these attacks, “average” defenses are hardly sufficient.

Has your organization in the past year been the victim of at least one spear phishing attack, where user credentials were compromised and/or fraud was committed?

- Yes: 46%
- No: 40%
- I don’t know: 14%

As noted earlier, 46 percent of respondents know their organizations were victims of at least one social engineering attack in the past year. But that number is likely to be inflated by some of the 14 percent who don’t know – or even the 40 percent who say no. If traditional tools are insufficient to detect and stop these schemes, then perhaps traditional perceptions about the prevalence of these schemes can be challenged, too.
If you answered “yes” the previous question, what business impacts did your organization experience as a result of the spear phising attack(s) and business email compromise? (check all that apply)

- Employee credentials were compromised: 65%
- Financial accounts were breached: 17%
- Intellectual property was breached: 15%
- We received negative publicity as a result of the attacks: 11%

For those respondents who said their organizations were victims, 65 percent say these attacks led to the compromise of employee credentials – the first step toward launching business email compromise strikes. Seventeen percent say financial accounts were breached, while 15 percent say intellectual property was compromised.

What do you believe to be your organization’s greatest vulnerabilities to spear phishing attacks? (check all that apply)

- Our user awareness efforts are ineffective: 50%
- Our current anti-spam and anti-virus technology is insufficient against today’s sophisticated attacks: 47%
- We cannot keep pace with the volume and sophistication of attacks: 38%
- Our business partners have insufficient security controls and/or user awareness: 31%
- We do not have senior management recognition and support that this is a serious problem: 12%

And what do security leaders blame for their organizations’ vulnerability to spear phishing attacks? Fifty percent say their own user awareness efforts are ineffective. But nearly as many – 47 percent – blame their current anti-spam and anti-virus technology, which frankly would be useless anyway against almost all social engineering attacks. This answer suggests that many security leaders are completely misreading the challenges associated with targeted attacks – which may be why 38 percent of respondents acknowledge that they cannot keep pace with the volume and sophistication of attacks.

The next section of the report reviews the attack volumes and types reported by respondents.
Attack Volumes & Types

The business criticality of social engineering attacks has been established. But what volume of attacks are organizations seeing, and is this substantially more than they saw in prior years? Two statistics to consider:

- 69 percent of respondents say the volume of attacks has increased in the past year;
- 88 percent say they have seen no change or an increase in financial losses associated with spear phishing incidents.

Check out the charts and numbers associated with volume and types of attacks.

How has the number of spear phishing incidents at your organization changed in the past year?

Consistent with what the FBI reports, 89 percent of respondents have seen either a steady pace or an increase in spear phishing and social engineering attacks in general in the past year. Very few report any degree of decrease.

Consistent with what the FBI reports, 89 percent of respondents have seen either a steady pace or an increase in social engineering attacks in the past year.
How have financial losses associated with spear phishing incidents at your organization changed in the past year?

- Increased substantially: 1%
- Increased slightly: 9%
- No change: 78%
- Decreased slightly: 5%
- Decreased substantially: 6%

Hand in hand with such incidents come fraud losses, and 88 percent of respondents say they have seen, again, either a steady pace or an increase in losses.

What percentage of attacks on your organization use spear phishing as a component?

- More than 50 percent: 7%
- Between 31 and 50 percent: 10%
- Between 21 and 30 percent: 9%
- Between 11 and 20 percent: 14%
- Under 10 percent: 21%
- I don't know: 38%

Asked “What percentage of attacks use spear phishing as a component?” 38 percent of respondents say they don’t know, while 21 percent peg the figure at under 10 percent. Forty percent put that figure at anywhere from 11 percent to over 50 percent.
Survey Results

What percentage of spear phishing attacks on your organization contain a malware-infected attachment or URL as a component?

- More than 50 percent: 25%
- Between 31 and 50 percent: 11%
- Between 21 and 30 percent: 9%
- Between 11 and 20 percent: 9%
- Under 10 percent: 16%
- I don’t know: 30%

Increasingly, organizations are seeing social engineering attacks that lack a malware component. Asked for a percentage of attacks that contain a malware component, 30 percent do not know, while one-quarter put that figure at more than 50 percent.

What are attackers seeking when they launch spear phishing attacks on your organization? (check all that apply)

- User credentials to commit fraud/theft against my organization: 69%
- Specific actions from the user, i.e., commit a fraudulent transfer of funds: 52%
- User credentials to commit fraud/theft against a third party: 27%

No surprise as to what attackers want. They are after user credentials to commit fraud against the organization, according to 69 percent of respondents. Fifty-two percent say the fraudsters are looking for the user to take specific actions, i.e., commit a fraudulent funds transfer, while 27 percent say the attackers use the compromised credentials to commit fraud or theft against a third party.

The report’s next section reviews responses related to trust & defenses.
Trust & Defenses

This section reviews the relative trustworthiness of email delivered to users, and details organizations’ current defenses against social engineering attacks. Among the responses:

- 22 percent do not know what percentage of email delivered to end users could be considered “untrustworthy.”
- 49 percent rate as average or below the effectiveness of the current controls they deploy to defend against social engineering attacks.

What percentage of the email that isn’t eliminated through your defense mechanisms and is delivered to your end users do you suspect to be untrustworthy?

So, how effective are current defense mechanisms in terms of filtering out what would be considered “bad” email? Only 13 percent of respondents say that their current defenses fail to filter out more than five percent of suspect emails. Another 13 percent peg that percentage at under three percent. Twenty-two percent do not know the answer.

Are you aware of situations where your organization or brand identity has been used in attempts to spear phish your customers or partners?

Brand spoofing is a significant component in modern targeted attacks, and respondents are split 40/40 over whether their organizations’ brands have been used in attacks on customers or partners. Twenty percent do not know the answer.
Is spear phishing a senior management/board level concern at your organization?

Asked whether social engineering is a senior management/board-level concern at their organizations, 70 percent of respondents say yes, while 12 percent do not know. Interestingly, 18 percent say it is not an issue, which begs the follow-up question “Why?”

Which of the following security controls do you currently have in place to defend against spear phishing attacks?

- Traditional anti-spam tools: 16%
- Email authentication to prevent spoofing from our own domains: 14%
- Traditional anti-virus tools: 12%
- Commercial anti-spear phishing solution: 10%
- URL filtering: 10%

Asked which security controls they have in place to defend against spear phishing attacks, 16 percent say “traditional anti-spam tools,” while 14 percent deploy email authentication to prevent spoofing from their own domains. Twelve percent list traditional anti-virus tools, which would have no impact whatsoever on socially engineered schemes.

These responses may well fuel the sentiment expressed in answer to the next question.
How do you assess the effectiveness of the controls you currently have in place to defend against spear phishing attacks?

A - Superior 8%
B - Above average 43%
C - Average 39%
D - Below average 9%
F - Failing 1%

Only eight percent of responses assess the effectiveness of their current controls as superior. And while 43 percent rate these controls as above average, 49 percent assess them at average or below.

In the next section, the responses will gauge confidence in business partners’ abilities to defend against these attacks.

Only eight percent of responses assess the effectiveness of their current controls as superior.
Partner Vulnerability

Seven percent is the key stat here – that’s how many respondents are “extremely confident” in their business partners’ abilities to defend against social engineering attacks that ultimately could compromise the respondents’ organizations.

Other responses:

On a scale of 1-4, what is your confidence in your business partners’ abilities to defend against spear phishing attacks that ultimately could also compromise your organization?

More than one-fifth of respondents say they have no confidence in their business partners’ abilities to defend against social engineering attacks that could impact the respondents’ organizations. Thirty-four percent say they are only somewhat confident, while 38 percent say they have no opinion either way.

So, if there is so much concern about partners, what are organizations doing about it?

More than one-fifth of respondents say they have no confidence in their business partners’ abilities to defend against social engineering attacks that could impact the respondents’ organizations.
Do you have a program in place to audit and encourage your partners who send your organization email to authenticate their email?

- Yes: 29%
- No: 50%
- I don't know: 21%

Nearly 30 percent of respondents say they have a program in place to audit and encourage partners to authenticate email sent to the respondents’ organization. Half say they do not have such a program, while one-fifth do not know.

Do you ask your partners to adopt email authentication practices such as DMARC?

- Yes: 23%
- No: 52%
- I don't know: 25%

The good news for DMARC proponents: 23 percent of respondents say they ask their partners to adopt email authentication practices such as DMARC – a strong turnout, given the relativeness newness of DMARC. Fifty-two percent do not have such a requirement, and the rest do not know.

Next, the report looks at the 2017 agenda to counter targeted social engineering attacks – where organizations will focus their new resources.
Countermeasure Agenda

The important information here: 98 percent of respondents expect the same or increased funding in 2017 to combat social engineering attacks. How will they invest these resources? See the following charts.

How do you expect your budget dedicated to anti-spear phishing to change in the next year?

- Increase of more than 10 percent: 11%
- Increase of 6-10 percent: 11%
- Increase of 1-5 percent: 29%
- No change: 47%
- Decrease: 2%

Social engineering attacks are enough of a boardroom/senior management issue that all but two percent of respondents say they will receive level or increased funding to combat the threat in 2017.

And of those who expect an increase, nearly one-third say it will be between one and five percent. Eleven percent expect greater than a 10 percent hike.

How will these funds be invested?

Social engineering attacks are enough of a boardroom/senior management issue that all but two percent of respondents say they will receive level or increased funding to combat the threat in 2017.
Sixty-six percent of respondents fall back on the crutch of “We’re going to invest more in staff awareness.” Which is fine if it’s effective training that helps users do a better job spotting and stopping the social engineering scams that are leading to compromised credentials. If it’s just “more of the same,” then the awareness dollars will be wasted investments.

Thirty-five percent say they will invest in email authentication to prevent spoofing from their own domains, while 30 percent are eyeing commercial solutions addressing social engineering.

Forty-five percent say they will invest in traditional anti-spam and anti-virus tools, which also runs the risk of being “more of the same.” It is clear that traditional tools have been ineffective against today’s prevalent attacks. Why would greater investment in these tools show different results?

It is no easy task to break from traditional approaches and try new tactics against social engineering attacks and the fraudsters who seek to compromise credentials. In the closing sections of this report, this challenge will be addressed by:

- **Conclusions** – which sum up the messages from the survey results
- **Analysis** – wherein John Wilson, Field CTO of survey sponsor Agari, offers his take on what these results mean and how security leaders can apply them to make a positive difference in their own organizations.
Conclusions

Before looking ahead to 2017, it is important to reflect on some of the resonant messages from survey respondents re: 2016. Namely:

• 60 percent of survey respondents say social engineering is one of the most significant threats they face today;
• 52 percent rate their organizations' defenses against social engineering attacks at average or below.

Corporate defenses currently are not up to the task of defending against the latest social engineering schemes, and this is a balance that must be shifted to prepare for the challenges of the year ahead.

Reviewing survey responses and the resonant messages from respondents, this report offers the following conclusions:

1. Make It a Management Issue

For the 30 percent of survey respondents who are unsure whether social engineering is or should be a senior management/board-level issue, it’s time to wake up to the FBI’s own stats: $3.1 billion in fraud losses in just under two years. A 1,300-percent increase. Organizations of all sizes – employees of all levels of seniority – are prime targets for attackers seeking credentials and privileged access. To paraphrase: All that’s necessary for the attackers to succeed is for good security leaders to say nothing. It’s time to make social engineering a top business issue.

2. Out with the Old

Forget traditional Secure Email Gateways (SEG) tools. They can’t hope to be effective at stopping or even spotting today’s social engineering strikes, many of which come without a malware component. Social engineering is the fraudster’s tool of choice today, and it’s consistently effective. To truly shore up defenses to at least attempt to keep pace with their adversaries, organizations need to explore new security solutions that verify that only trusted emails from legitimate senders reach users’ inboxes, whether or not there is malware or malicious URLs in the message.

3. Awareness, Yes, But

Just as traditional security controls don’t cut it against today’s social engineering schemes, neither do some of the more common forms of user training. Many organizations continue to conduct internal phishing attempts, and most employees have been drilled incessantly about resisting the urge to click on questionable links or open unknown email attachments. But with so many of today’s attacks relying on targeted social engineering, users simply will not be able to consistently distinguish legitimate emails from malicious ones. Users should not be relied upon as a defense to social engineering, spear phishing or business email compromise. To protect organizations, security controls should prevent untrusted email from being delivered to inboxes.

4. It’s About Trust and Authentication

John Wilson, Field CTO of survey sponsor Agari, explores this topic at length in the analysis that closes this report. The critical component to protecting against social engineering, spear phishing and business email compromise is the ability to validate that the purported sender is truly the person messaging you. To protect your employees from receiving email spoofing your own domain, DMARC-based authentication of inbound email will be most effective. For attacks that impersonate any other brand or domain, it is important to implement technology that analyzes the trust and authenticity of inbound email messages.

NOTE: In preparation of this report, ISMG VP Tom Field sat down with John Wilson, Field CTO at survey sponsor Agari, to analyze the results and discuss how security leaders can put these findings to work in their organizations. Following is an excerpt of that conversation.

Board-Level Issue

TOM FIELD: One of the thing that jumps out to me is that 70 percent of our survey respondents say that social engineering is a board-level issue. My question is, what are the other 30 percent overlooking?

JOHN WILSON: Actually, 12 percent of the respondents said they didn’t know whether social engineering is a board-level issue. So, it’s really only the 18 percent who said “no,” that I’m worried about. Now I will tell you this: Once somebody wires a half-million dollars to an offshore account, I promise you that social engineering will very quickly become a board-level concern.

Validation & Surprise

FIELD: In what ways do these survey results validate your beliefs about social engineering across the different industry sectors?

WILSON: Social engineering impacts every type of business, regardless of company size, sector, or even location. Every time we install our Enterprise Protect solution at a client site, we almost immediately will find at least one or two CEO wire fraud attempts. We’ve even received these ourselves. So the fact that only five percent of respondents don’t consider social engineering to be a threat pretty much validates our beliefs, because obviously the other 95 percent do perceive it to be some degree of threat.

FIELD: In what ways do the survey results surprise you?

WILSON: I was particularly surprised to see that 21 percent of respondents believe that less than 10 percent of attacks on their company use social engineering as a component of the attack. This flies in the face of many other studies, most notably the Verizon Data Breach Investigations Report, which consistently shows that social engineering is a component in the vast majority of breaches.
When most companies look at attacks, they think about things like SQL injections, data breaches or DDoS attacks. Although social engineering certainly is not a component in a DDoS attack, it very often is in the case of a breach. Too often, companies don’t initially know the cause of a breach, and it’s only much later that they will trace things back and realize that it was, in fact, related to a social engineering message.

**Vulnerability**

FIELD: Half of the respondents say that their greatest vulnerability is that their user awareness efforts are ineffective. Now I know sometimes that people just use user awareness as kind of a crutch. “Our awareness is bad; we need to put more money here.” But, again, what are they overlooking?

WILSON: Yes, well, 47 percent also said that their current anti-spam, anti-virus solution wasn’t up to the task. Thirty-eight percent said they couldn’t keep pace with the volume and sophistication of the attack. So I think the results show that people understand there is no single vulnerability which, if eliminated, would solve this intractable problem. So it really comes down to the fact that this is very complex and that no one thing, be it user awareness, be it an anti-virus solution, is going to solve this problem.

“If our defenses were sufficient, social engineering attacks would no longer be a significant business threat.”

**Social Engineering**

FIELD: So many email-borne exploits these days come without a malware component. What trends are you seeing in the market regarding pure social engineering? And how can organizations best respond?

WILSON: We are seeing an increase in the sophistication as well as the diversity of the attacks. The advent of social networking has made it very easy for criminals to research information that they may then leverage through social engineering. In the days of a Kevin Mitnick, he was dumpster-diving behind a company to come up with a couple of names of an employee, so he had an edge when he made a phone call to that organization. Those days are gone. You don’t have to do that anymore. You can simply go to sites like LinkedIn, or even a company’s “Management” page to do all of the intel you need to run one of these attacks. And while the CEO wire fraud and W-2 fraud examples make the headlines, it’s really the unique attacks that scare me the most.

For example, we recently had a customer experience several attempts to get their AWS credentials via a series of targeted email messages. Now these messages easily evaded their spam filter, yet our solution had no trouble identifying them. And that’s because most spam filters look for the needle in a haystack, which is fine, so long as the needle looks exactly like what you would expect to see. However, not all needles look alike. Our solution identifies the hay. The hay always looks the same, and it turns out, if you find the hay, you know that everything else has to be a needle.

As for a response, companies need a three-pronged approach to this problem. You need to educate your employees. You need a technology solution that is purpose-built to detect targeted attacks, so not just your run-of-the-mill spam filter, but rather something that is designed specifically for this challenge. And, finally, please implement DMARC. It’s a standard that will ensure that nobody can spoof your corporate domain in the front header of an email message.
Third-Party Risks

FIELD: What do you see as a growing risk from third parties? And, again, how can organizations best respond?

WILSON: As companies outsource functions that were traditionally performed in-house, the attack surface has grown much larger. For example, if you perform your own payroll function in-house, you just need to worry that your payroll team is trained and well aware of social engineering. But as soon as you outsource your payroll, that attack surface grows to now include anyone at your payroll provider and possibly anybody who subcontracts to that payroll provider – basically anyone who has access to your employees’ data. So companies can mitigate these risks a number of ways. One highly effective tool is DMARC. As I’ve mentioned it before, you’re going to probably hear this as a recurring theme throughout this interview: DMARC is a standard that can ensure the authenticity of email communications.

DMARC

FIELD: We asked our respondents about DMARC. How encouraged are you by what they tell us about their adoption rates?

WILSON: Adoption of the DMARC standard has far exceeded my expectations. Ninety percent of U.S. consumers receive their email at a provider who enforces the sender’s DMARC policy. I can’t think of any other optional Internet standard that has had that much traction after just 4.5 years. Sender adoption has been somewhat slower, but it’s starting to reach critical mass, and some of the most phished, most spoofed names on the planet – a lot of banks, social networks – they have traditionally been the bait, if you will, in these scams, and they, by and large, have stood up, implemented DMARC, and have seen a marked decrease in their brand being used out in the wild to target people.
2017: A Look Ahead

FIELD: As we look ahead to the coming year, what are the social engineering trends that really give you the most concern?

WILSON: I’m really worried that criminals will become more creative. Every CISO is aware that criminals will pose as their CEO in order to get employee W-2 information or to initiate a wire transfer. They’ve trained their HR and finance teams to be on the lookout for these scams, and the criminal keeps running the same play day after day. I guess there’s always somebody who just didn’t quite get the memo yet. But as the criminals step up their game and they make the ruse a little bit more elaborate, I think that we’re going to see that things are going to start to get really, really scary. They’re not just going to be going after the HR department and the finance team. They’re going to go in through the side door, work their way through the company, and then, ultimately, compromise some group admin’s email account, so they can then request a wire transfer from within the company network. And, chances are, that group admin hasn’t had the same level of training against spear phishing as the finance team or the HR team. So that’s what really scares me. Criminals today are really on version 1.0 of their scam, and when they start to refine that, we’re all going to be in a lot of trouble.

“While the CEO wire fraud and W-2 fraud examples make the headlines, it’s really the unique attacks that scare me the most.”

Key Investments

FIELD: So, as we get into versions 2.0 and 3.0, what then become the defensive investments that make the most sense?

WILSON: Adopt DMARC. Start by publishing a monitor policy, so that you understand where your mail comes from and whether or not it’s properly authenticated. Then the way the journey with DMARC works is you fix up any non-compliant mail streams. You implement the authentication on those streams that are not currently authenticated. And, finally, once you have control over all your outbound email, you implement a reject policy, and, at that point, nobody can spoof your domain.

Now DMARC is an open standard. You can do it yourself, or you can work with a vendor. Agari has helped many of the best-known brands in the world take back control of their email channel, and we offer a technology platform and the subject matter expertise needed to ensure a successful DMARC implementation. That is, without question, one of the best things you can do because what it means is nobody can now spoof your CEO’s exact email address or the exact email address of any other employee, for that matter, and nobody can use you as the bait to trick one of your customers, partners or vendors. And if everybody did their part by implementing DMARC, the world really would be a much better place. The criminals would have a much more difficult time perpetrating these scams.

The Awareness Crutch

FIELD: We know that awareness enough is not going to solve this. How do we help organizations get over that perception that awareness is the panacea?

WILSON: My mom knows, of course, what I do for a living, and a frequent topic of my conversation with her is the latest scam that I’ve seen. I’m always just super worried that she’s going to fall for one of these things, but I’m always telling her “be on the lookout for this, be on the lookout for that.” I’ve given her all of the tips again and again. Yet one day, she received an email message from her choir director, and she actually did what I told her to do. She checked the email...
address, and it was right. This particular message, by the way, had a link to a Google doc that said, “Oh, you have to see this, it’s very funny.” Which she thought was a little bit out of character for her choir director to be sending. In any case, she looked at the headers even – I showed her how to do that – and she saw that this message passed authentication. And so she figured, “Well, you know, it must be real.”

But then she remembered the last thing I said, which was: When in doubt, reach out to the person and ask if they really sent this. Which would have been great if she’d picked up the phone to do that. Unfortunately, she did not pick up the telephone; she simply replied to the email and said, “What is this all about? Did you really send me this message?”

Well, what had happened is the choir director had been phished out of her credentials, and her email account was compromised. The criminal got logged in there, changed the password so the choir director couldn’t get in anymore, and now was sending all sorts of things to all of the choir director’s contacts. Well, my mom’s message arrived. The criminal posing as the choir director, said “Oh, yeah, absolutely; you’re going to laugh yourself silly.” So my mom clicked the link. It then asked for her Google credentials so she could view the document. Well, again, she was a little suspicious, but she’d just gotten an email back from the choir director, so in go the credentials.

Anyway, about 15 minutes later, I discovered this whole scam when I received a message from my mom, saying, “Open this; you’re going to laugh your pants off,” and, of course, I immediately knew what had happened. I called my mom. She realized, at that point, she was locked out of her account, etc. So this long-winded story really goes to show that you can have as much awareness as possible. I guarantee you that, for her age bracket and her location, my mom is one of the most aware people of any of these scams, and yet she did manage to get fooled. Sadly, some people just will not get over the fallacy that perception alone will solve the problem, until after they’ve suffered a successful attack.

“Put in some sort of anti-spear phishing technology, something that goes above and beyond what a normal spam filter does, something that is designed specifically to find these new attacks.”

Survey Results in Action

FIELD: How do you recommend that our audience best put these survey results to work in their organizations?

WILSON: Well, only 10 percent of respondents felt that their defenses were below average or failing, while 51 percent felt that their defenses were above average or superior. And I think that’s really similar to the statistics that say that 80 percent of drivers believe they are better than average drivers. I think we all realize there’s a fallacy in that, obviously, as that half of the world can be better than average. That’s kind of the definition of average. So I hope that the survey has helped practitioners realize that there is no single silver bullet to the spear phishing problem. People need to invest in a variety of solutions. If I could only do one thing, I would do DMARC. However, putting in some effort in employee training is certainly recommended as well. That certainly should not be the only thing you do. And then, finally, put in some sort of anti-spear phishing technology, something that goes above and beyond what a normal spam filter does, something that is designed specifically to find these new attacks.
About ISMG

Information Security Media Group (ISMG) is the world’s largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from the North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401
sales@ismgcorp.com